21-MJ-7141-JCB

AFFIDAVIT OF POSTAL INSPECTOR ZACHARY DAVIES IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Zachary Davies, a Postal Inspector with the United States Postal Service, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Postal Inspector with the United States Postal Inspection Service ("USPIS") since November 2017. I am assigned to the Mail Fraud and Crimes against Children Team of the USPIS's Boston Division. I am authorized to investigate violations of United States law and to execute warrants issued under the authority of the United States. I have received training in conducting investigations of crimes that adversely affect, or fraudulently use, the United States mail and the United States Postal Service ("USPS"). I have participated in criminal investigations of various violations of Title 18 of the United States Code involving financial crimes, including mail, bank and wire fraud, identity theft, money laundering, and computer crimes to include crimes against children.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the residential premises of 86 Marlborough Street, Apartment 27, Lowell, Massachusetts, 01851 (the "SUBJECT PREMISES"), as more fully described in Attachment A, which is incorporated herein by reference. As described herein, there is probable cause to believe that the SUBJECT PREMISES contains contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(a)(5)(B) (possession and distribution of child pornography), which items are more specifically described in Attachment B, which is also incorporated herein by reference.

3. The statements in this affidavit are based in part on information provided by federal agents; written reports about this investigation that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of subpoenas; the results of physical surveillance conducted by law enforcement agents; independent investigation and analysis by federal agents/analysts; and my experience, training, and background as a Postal Inspector with USPIS.

4. Because this affidavit is submitted for the limited purpose of securing the requested search warrant, I have not included every fact known to me concerning this investigation. Instead, I have set forth only those facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES.

PROBABLE CAUSE

Mailing of Child Pornography

5. On March 2, 2021, during a routine screening of incoming mail, investigators at Federal Correctional Institution Elkton ("FCI Elkton") discovered printed out images that included sexually explicit depictions of children, within a package addressed to an FCI Elkton inmate ("PERSON 1"). The package included the following return address information: The Rainbow Times, LLC, Quincy, MA 02169. The package also had a sticker with the following USPS tracking number: 9549010992531057038893.

6. On March 3, 2021, an investigator from FCI Elkton contacted the Cleveland Division of the Federal Bureau of Investigation's Child Exploitation Task Force to report the aforementioned package.[1]

7. On March 11, 2021, law enforcement examined the package and determined that the sender had enclosed eight, separate photographs of children within five different magazines. While the mailing address on four of the magazines appears to have been removed, the mailing address on one of the magazines was included: Jason M. Godin, Apt. 27, 86 Marlborough St., Lowell, MA 01851-3063, which is the SUBJECT PREMISES. It appears that the images had been printed with a photo printer and that the sender tried to hide the printouts within the magazines. I have reviewed the following printouts that had been hidden inside the magazines[2]:

[1] FCI Elkton is located in the Northern District of Ohio, Eastern Division.

[2] To avoid unnecessary in-person interaction given the health concerns posed by the current pandemic, I am not providing a copy of these images to the Court. I am aware that the "preferred practice" in the First Circuit is that a magistrate judge view images that agents believe constitute child pornography by virtue of their lascivious exhibition of a child's genitals. *United States v. Brunette*, 256 F.3d 14, 18-19 (1st Cir. 2001). Here, however, the description offered "convey[s] to the magistrate more than [my] mere opinion that the imag[e] constitute[s] child pornography." *United States v. Burdulis*, 753 F. 3d 255, 261 (1st Cir. 2014) (distinguishing Brunette). The description of certain images here is sufficiently specific as to the age and appearance of the alleged child and the type of sexual conduct he is engaged in that the Court need not view the file to find that it depicts child pornography. *See United States v. Syphers*, 426 F.3d 461, 467 (1st Cir. 2005) ("The best practice is for an applicant seeking a warrant based on images of alleged child pornography is for an applicant to append the images *or provide a sufficiently specific description of the images* to enable the magistrate judge to determine independently whether they probably depict real children.") (emphasis added). For example, the image described in Paragraph 7(h) clearly depicts a child well under 18 engaging in oral sex, which clearly constitutes child pornography.

a. A color printout found within a "Better Homes & Gardens" magazine, which depicts a prepubescent male approximately 8 to 12 years old wearing a blue speedo leaning against a rock. The printout was attached to a leaflet insert.

b. A color printout found within a "Boston Home" magazine, which depicts a prepubescent male approximately 4 to 7 years old wearing only a white tank top with red edging, with his penis exposed to the camera

c. A color printout found within a "Boston Home" magazine, which depicts a nude prepubescent male approximately 4 to 7 years old lying face down on a bed with his buttock and scrotum visible. Both printouts were attached to leaflet inserts.

d. A color printout found within a "Food Network" magazine, which depicts a prepubescent male approximately 8 to 12 years old posing for a camera wearing a dark-blue speedo-style bathing suit. The printout was attached to a leaflet insert.

e. A color printout found within a "Boston Home" magazine, which depicts a nude prepubescent male approximately 4 to 7 years old lying on his back in a black office chair, holding his buttocks apart and exposing his anus to the camera. The child is wearing black headphones. The letters "pydo" and a flame-like object are in purple on the lower right-hand corner of the printout.

f. A color printout found within a "Boston Home" magazine, which depicts two nude prepubescent males approximately 4 to 7 years old leaning backward in a seated position toward each other. Each child is holding his exposed, erect penis. Both photos were attached to leaflet inserts. A label on the cover of the magazine listed the recipient as: Jason M. Godin, Apt. 27, 86 Marlborough St., Lowell, MA 01851-3063, which is the SUBJECT PREMISES.

g. A color printout found within a "Better Homes & Gardens" magazine, which depicts a nude prepubescent male approximately 8 to 12 years old seated, leaning backward on a brown couch. The child is holding his exposed, erect penis. The printout was attached to a leaflet insert.

h. A color printout found within a "Better Homes & Gardens" magazine, which depicts a prepubescent male approximately 3 to 7 years old performing oral sex on an adult. The printout was attached to a leaflet insert.

Further Investigation

Jason Godin and PERSON 1

8. On October 12, 2016, Jason M. GODIN ("GODIN") pled guilty in the United States District Court for the District of New Hampshire to a one-count information charging Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). On March 16, 2017, United States District Court Judge, Steven J. McAuliffe sentenced GODIN to 36 months in prison and 10 years of supervised release. According to BOP records, GODIN was incarcerated at FCI Elkton from April 14, 2017 to June 11, 2019. At this time, GODIN remains on supervised release. He is being supervised by the United States Probation and Pretrial Services Office for the District of Massachusetts ("U.S. Probation"). Based on conversations with U.S. Probation, I understand that GODIN is currently being monitored at this address. I similarly understand that if GODIN were to change addresses, he would need to report his new address to U.S. Probation.

9. Based on a review of a law enforcement database, I understand that GODIN has an active Massachusetts Driver's License and that he listed the SUBJECT PREMISES as both his

mailing and residential address. I similarly understand that GODIN has a motor vehicle that has an active registration associated with the SUBJECT PREMISES.

10. On March 22, 2021, I conducted physical surveillance at the SUBJECT PREMISES. I neither observed GODIN nor his motor vehicle. I entered the apartment building and observed a mailbox for apartment 27 that did not have a listed name. Outside the door to the SUBJECT PREMISES, I observed a rock that had "The Godins" printed on it.

11. According to FCI Elkton records, beginning on or about August 9, 2017, GODIN and PERSON 1 shared a cell at FCI Elkton for approximately two years. As described above, the USPS package containing child pornography was addressed to PERSON 1, and one of the magazines enclosed in the package listed GODIN as the original recipient.

12. In connection with the investigation, I have reviewed an undated, anonymous letter that was received by investigators at FCI Elkton on or about March 15, 2021. The letter appears to have been written by an inmate at FCI Elkton and details, among other things, the relationship between GODIN and PERSON 1: "I'm guessing you are already aware of inmate [PERSON 1] from FSC using the mail & magazines to get in illegal porn. If you have the package, he told others that his ex J. Godin (former inmate & on US Prob) was mailing these items in. The postmark would likely be that of Godin's address." The letter further details the distribution of pornography within FCI Elkton.

Mailing of the USPS Package to PERSON 1

13. Through a review of USPS and open source databases, a USPIS investigative analyst determined the following information related to the shipping of the USPS package addressed to PERSON 1 with tracking number 9549010992531057038893: (1) it was shipped from a United States Post Office located in Lowell, Massachusetts, on February

26, 2021 between 4:01 PM and 4:02 PM.; (2) it cost $4.01 to ship the package and it was paid for with a debit card ending in xxxxxxxxxxxx9194 ("x9194") maintained at Customers Bank.

14. I have reviewed records produced by Customers Bank that are associated with the debit card x9194.[3] This debit card is linked to deposit account number xxxxxx2980 ("x2980"). GODIN is listed as the account holder for "x2980 and the SUBJECT PREMISES is listed as his address. An account statement for February 2021 confirms that on February 26, 2021 at 4:02PM, a "POS Purchase Pin transaction" using x9194 for $4.01 took place at "USPS PO 24216508 Lowell MA."

15. In connection with investigation, I have obtained and reviewed surveillance footage from the Lowell Post Office branch on the date and time when the package addressed to PERSON 1 was mailed. The footage reflects a male dressed in a grey hoodie, grey sneakers, and winter hat mailing a package consistent with the package addressed to PERSON 1.

16. On March 25, 2021, I met with the U.S. Probation officer assigned to supervise GODIN and showed him the surveillance footage described above. The U.S. Probation officer has had numerous contacts with GODIN, both in person and via virtual meetings. After reviewing the footage, the Probation Officer opined that the individual mailing the package could be GODIN but that he was not 100 percent certain because the individual was wearing a hat and mask. The U.S. Probation officer noted that that the individual in the video was wearing a pair of sneakers that he had seen GODIN wear in the past.

[3] Based on my review of the bank records, I believe that the account is a "T-Mobile Money" checking account associated with the "BankMobile Division Customers Bank."

Electronic Devices

17. In connection with the conditions of his supervised release, GODIN must report to U.S. Probation all electronic devices that he uses to access the internet. Probation is then able to conduct periodic spot-checks to evaluate GODIN's internet use on a certain date and time. To date, GODIN has only disclosed an Android phone and U.S. Probation has not found any review of child pornography associated with this device.

18. Accordingly, I am continuing to investigate how GODIN accessed, and possibly, printed out, the images that I have reason to believe that he sent to PERSON 1. Based on my training and experience, I believe that GODIN may have one or more other electronic devices in his possession that he has not disclosed to Probation and that he may be using to access and/or print child pornography.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

17. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute, or access with intent to view child pornography (collectively, "consumers" of child pornography) have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to such consumers of child pornography, as outlined in the following paragraphs.

18. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

19. Consumers of child pornography may collect sexually explicit materials, which may consist of hard copy and digital images and videos for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

20. Many consumers of child pornography maintain their sexually explicit materials for several years and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.[4] They regularly maintain their collections in the privacy and security of their homes, inside their cars, on their person, or in cloud-based

[4] *See United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

online storage.[5] Depending on their technical expertise, access to child pornography on seemingly "safe" networks like Tor, or struggle with addiction to child pornography, many consumers of child pornography have been found to download, view, and then delete child pornography on their digital devices on a cyclical and repetitive basis.

21. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[6]

22. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate

---

[5] I and/or my colleagues have been involved in investigations where, for example, an offender who lived with his parents kept a laptop with child pornography in the trunk of his car; an offender who lived with his parents and sister maintained his child pornography and communications with minors in a cloud-based application that he accessed from multiple phones (one of which he secreted in his work vehicle when he realized law enforcement was searching his home) and tablets; and countless offenders who kept thumb drives and digital devices in various locations throughout their homes.

[6] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging applications, and other similar vehicles of communication.

23. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.

24. Based upon training and experience, I know that persons engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

25. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, including on digital devices

other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

26. Based on the facts outlined herein, I believe that a user of the internet at the SUBJECT PREMISES likely shares some or all of the characteristics of consumers of child pornography described above.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

27. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable, or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown

tremendously within the last several years. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

e. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

f. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

information can be intentional, *i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

g. Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence, suspects, or victims. For example, the file data for images stored on a computer may provide geolocation information or information indicating when the file or image was created.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable

media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

30. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little to no cost.

b. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." An internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

31. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and

the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

32. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

33. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

34. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

36. Based on my knowledge and training and the experience of other agents with whom I have spoken, I know that in order to completely and accurately retrieve data maintained on

computer hardware, computer software, and storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true due to:

a. The volume of evidence—storage media such as computers, cellphones, tablets, hard disks, external storage devices, flash drives, CDs and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements--analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in

unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

37. The SUBJECT PREMISES may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

38. The law enforcement agents will endeavor to search and seize only the computer equipment that, upon reasonable inspection or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize

a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

40. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. Review of this electronic data may be conducted by any government personnel assisting in the investigation, including law enforcement officers and agents, attorneys for the government, attorney support staff and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

41. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

42. The passcode(s) that would unlock the mobile device(s) that may be present at the SUBJECT PREMISES are not currently known to law enforcement. Thus, it may be useful to press an individual's finger(s) to the devices' fingerprint sensor or to hold the device up to his face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data

contained on those devices for the purpose of executing the search authorized by this warrant.

43. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals present at the SUBJECT PREMISES to the sensor of the devices or place the devices in front of his face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

44. Based on all of the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(a)(5)(B) (possession and distribution of child pornography), as described in Attachment B, are located at the SUBJECT PREMISES, as more fully described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

Sworn to under the pains and penalties of perjury,

Zachary Davies

Zachary Davies
Postal Inspector
United States Postal Inspection Services

Sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 on May 4, 2021.

HON. JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is located at 86 Marlborough Street, Apartment 27, Lowell, Massachusetts, 01851. The SUBJECT PREMISES is located within an apartment building which is brick with white trim. The apartment building, and in turn, the SUBJECT PREMISES, is accessed by a green door with the number "86" affixed to it. The SUBJECT PREMISES is located at the top of a flight of stairs. The number "27" is attached to a grey door outside the SUBJECT PREMISES. The exterior of the apartment building and the SUBJECT PREMISES are pictured below:

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(a)(5)(B) (possession and distribution of child pornography), including:

A. Records relating to the following topics:

1. Child pornography;

2. The sexual abuse or exploitation of children;

3. Child erotica;

4. The identity of any child depicted in videos and photographs located in the equipment or discussed in any communications related to child pornography or the sexual abuse or exploitation of children;

5. Communications that relate to the sexual exploitation of children;

6. Internet activity reflecting a sexual interest in minors or child pornography; and

7. Membership in online groups, clubs, or services that provide, make accessible, or otherwise concern child pornography.

B. Any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment.

C. Records relating to any social media account(s) or communication application(s) used to send or receive any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment.

D. Records relating to or referencing PERSON 1, an inmate at FCI Elkton whose identity is known to the affiant.

E. Records relating to Customers Bank debit card xxxxxxxxxxxx9194 and/or account xxxxxx2980.

F. Any issue(s) of Better Homes & Gardens magazine, Boston Home magazine, or Food Network magazine, and/or any records relating to any subscription to or purchase of any such magazine.

G. Correspondence sent to or received from FCI Elkton, and/or any records relating to such correspondence.

H. Records relating to the identity, location, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above.

I. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter forensic programs and associated data that are designed to eliminate data;

5. evidence indicating how and when the computer equipment was accessed or used;

6. records of or information about any Internet Protocol addresses used;

7. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

8. records and tangible objects pertaining to accounts held with companies providing internet access or remote storage of either data or storage media;

9. records of or information about the computer equipment's internet activity; and

10. contextual information necessary to understand the evidence described in this attachment.

J. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and

K. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

III. During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals to the sensor of the mobile device(s) seized pursuant to this warrant and/or to hold such device(s) in front of his/her face.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related

items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. "Child Pornography," as defined in 18 U.S.C. § 2256(8)(A), means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

I. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

EXECUTION

Searching agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence authorized by this warrant, as outlined above. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of

victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If the computer equipment contains contraband, it will not be returned. If the computer equipment cannot be returned, agents will attempt to make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.